INCEIF UNIVERSITY

Tender for the Supply, Design, Development, Testing, Commissioning, Training and Support of the National Islamic Social Finance Data Repository (NISFR)

Tender No.: INCEIF/NISFR 1/2026

Appendix A – Executive Summary

1. Background

Islamic social finance (ISF) in Malaysia – including zakat, waqf, sadaqah and related programmes – is delivered by many institutions across states and sectors. Each institution keeps its own records in its own systems and formats. As a result there is no trusted, consistent national view of what is being delivered, to whom, where and with what outcome.

INCEIF University intends to establish the **National Islamic Social Finance Data Repository (NISFR)**: a trusted national data infrastructure that provides a common data standard and a controlled way for participating institutions to submit agreed data, have it validated, and obtain useful national, state, sector and institutional insight – **without replacing institutional operational systems or displacing statutory ownership and authority**.

2. Objectives

- Establish a common, version-controlled **National ISF Data Dictionary and taxonomy** in Bahasa Melayu and English.
- Give contributing institutions a **secure, simple way to submit data** by guided web forms or standard XLSX/CSV templates.
- Ensure data quality through **validation, attestation and data-steward review** before anything is published.
- Publish **authoritative statistics** that come only from governed repository data, with clear source, period and status.
- Protect privacy and institutional confidentiality through **access tiers, disclosure controls and a tamper-evident audit trail**.
- Deliver a platform that INCEIF **owns, can operate and can move**, with full documentation and handover.

3. What the Project will deliver

The Project will be delivered in multiple releases under one contract. The first release delivers the **Base Scope** defined in Appendix B – all requirements marked as Base Scope, together with the required deliverables. In summary:

Area	What is delivered
Platform and portal	A secure, bilingual (BM/EN) national NISFR platform with a public website for approved statistics, metadata, resources, help and service information, and an institutional portal
Users and institutions	User lifecycle management with multi-factor authentication; role- and institution-scoped access; onboarding of contributing institutions and reporting units; programme master data and reporting periods

Area	What is delivered
Data submission	Guided web forms and controlled XLSX/CSV template upload (including bulk upload) using the approved data dictionary and taxonomy
Validation and review	Configurable validation (completeness, format, taxonomy, cross-field, privacy, duplicates); attestation; data-steward review, clarification and decision history; approval and publication workflow with segregation of duties
Governance and trust	Access tiers and disclosure controls including primary and secondary small-cell suppression; versioning and provenance of every governed value; tamper-evident audit trail; notifications and reminders; system configuration
Insight	An initial set of national, state/sector and institutional dashboards, a data explorer with predefined filters, standard reports and exports, and data-quality scorecards – embedded in the NISFR portal
Service and handover	Security, monitoring, backup and recovery; four separate environments; training, documentation, knowledge transfer and 12 months of warranty and support after go-live

Some Base Scope requirements are delivered to a defined scope in this release (for example, the initial dashboard set and standard reports). The exact scope of each requirement is stated in Appendix B.

4. What the Project will not do

- Migrate historical data, or replace institutional source, payment/disbursement or beneficiary case-management systems.
- Build API or other system-to-system integration with institutional or government systems. Institutions submit data by web form or template upload.
- Change statutory mandates, ownership or institutional decision rights.
- Store direct beneficiary identifiers such as name, MyKad/passport number, phone, email or full address. Pseudonymised data remains subject to privacy obligations.
- Publicly release restricted or confidential data, or data that could identify small groups.
- Make automated policy or individual eligibility decisions.

5. Scope at a glance

Category	Requirements (see Appendix B for detail)
Base Scope (in the fixed price)	Platform, portal, user and role management, institution onboarding, programme management, data entry and upload, validation, privacy by design, submission workflow, steward operations, taxonomy and dictionary, access and disclosure control, versioning and provenance, audit trail, notifications, configuration, bilingual and accessible user experience Data quality, dashboards, data explorer and reports and export, to the scope defined in Appendix B All security, hosting, performance, availability, environment, portability, monitoring and implementation requirements
Post Go-Live Scope (in the fixed price; delivered within 3 months after go-live, on dates the Tenderer proposes)	Advanced analytics; Knowledge Hub; subscription and payment; identified beneficiary data module (switched off until INCEIF approves activation)

Category	Requirements (see Appendix B for detail)
Priced Options (INCEIF may commission)	Benchmarking; controlled data access; single sign-on; AI-assisted insight (Ask ISF) Institutional APIs / government data exchanges; I-FIKR integration

Every Priced Option must be priced in Appendix E; a Commercial Proposal that omits one is incomplete.

6. Key facts and service baseline

Users and roles	Public; registered researcher/professional; data officer; focal person; responsible officer; policy user; data steward; repository administrator; auditor
Capacity baseline	300 contributing institutions; 5,000 registered users; 20,000 programmes; up to 10 million approved pseudonymised records over five years
Availability and recovery	At least 99.5% monthly production availability; recovery point objective 24 hours; recovery time objective 8 hours; tested backup and disaster recovery
Hosting	Production services and backups hosted in Malaysia, in a cloud platform subscription owned by INCEIF. The Contractor deploys and operates the solution in that subscription; cloud consumption is paid by INCEIF
Environments	Separate development, test/UAT, staging and production; no unmasked production data in lower environments
Analytics	Dashboards, data explorer and reports delivered within the NISFR portal, so that institutions and the public do not need individual licences
Language and accessibility	Bahasa Melayu and English throughout; WCAG 2.2 AA
Ownership and portability	INCEIF-controlled accounts; source code owned by INCEIF; full documentation; full data export in open formats (e.g. CSV, JSON)
Server sizing	Appendix C gives a go-live starting point and a scale-up reference. Tenderers propose and justify their own sizing, proven by load testing

7. Delivery approach and indicative timeline

The Contractor delivers discovery and design, build, testing (system integration, user acceptance, security, performance and accessibility), a **pilot with selected institutions covering at least one validated reporting cycle**, deployment, training, documentation, knowledge transfer and 12 months of warranty and support. INCEIF appoints the independent penetration tester and accessibility auditor.

Milestone	Indicative timing
Contract award (Letter of Award)	By 31 December 2026
Contractor mobilises	4 January 2027
Discovery, design baseline and environments	January 2027
Build	January – April 2027
System integration, security, performance and accessibility testing	April – May 2027
User acceptance testing and pilot (one validated reporting cycle)	May – June 2027

Milestone	Indicative timing
Go-live	**No later than 30 June 2027**
Warranty and support	12 months after go-live
Post Go-Live Scope delivery	After go-live, within 3 months after go-live date

The go-live date is fixed. Tenderers must show in their technical proposal (Appendix D) a resource-loaded plan and a named team available to start in early January 2027. Contractual milestones, payment and acceptance terms are set out in the Tender Document.

8. Project governance

- INCEIF governs the Project through a **Project Steering Committee** and a designated project lead.
- An INCEIF **product owner** and **data stewards** take part in design sessions and sprint reviews; contributing institutions take part in testing and the pilot.
- The Contractor provides a project director and a project manager, and reports progress, risks and changes to INCEIF as set out in the Tender Document.
- Acceptance is against the criteria in the Tender Document and Appendix B, including the go-live gate (pilot onboarded and governed; UAT, security and privacy tests passed).

9. Key tender dates

Step	Date
Invitation to Tender issued and tender advertised	Monday 23 November 2026
Last day to submit the Acknowledgement to Participate (Form A1) and the signed Undertaking of Confidentiality (Appendix F)	Friday 27 November 2026
Tender documents released to Tenderers who have signed	24 – 30 November 2026
Tender briefing (optional) – in person at INCEIF	Tuesday 1 December 2026, 11.30 am
Last day for written clarification questions	Thursday 3 December 2026, 12.00 noon
Clarification responses and any addenda issued to all Tenderers	Friday 4 December 2026
Tender closing	**Tuesday 8 December 2026, 4.00 pm**
Technical presentations and live demonstration (as invited)	10 – 14 December 2026
Tender evaluation (indicative)	9 – 22 December 2026
Tender award – Letter of Award (target)	By 31 December 2026
Commencement of contract	Monday 4 January 2027

Dates other than the closing date are indicative; any change is confirmed by addendum.

10. Contents of the tender pack

Document	Purpose
Tender Document	Instructions, evaluation, scope, implementation and acceptance, support and conditions of contract
Appendix A – Executive Summary	This overview (for information only)
Appendix B – Functional Requirements	All requirements, compliance matrix, data dictionary and templates (confidential)
Appendix C – Suggested Server Specifications	Indicative hosting and sizing reference
Appendix D – Technical Proposal Template	Required structure of the technical proposal
Appendix E – Commercial Template	Pricing for Base Scope, Priced Options and support
Appendix F – Undertaking of Confidentiality	Signed and returned before documents are released
Appendix G – Submission Note	Submission checklist and declaration
Attachment 1 – Tender Forms A1 to A4	Acknowledgement, business info, integrity, checklist

Enquiries

Enquiries must be made in writing, quoting Tender No. INCEIF/NISFR 1/2026, to **the IERIF 510 Project Team, ierif510@inceif.edu.my, +603 7651 4028**. Do not contact other INCEIF staff about this tender.